

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Інв. № ориг.	
Підп. та дата	
Взам. інв. №	
Інв. № дубл	
Підп. та дата	

Центр сертифікації ключів
ринку електричної енергії

Загальний опис системи

ЄААД.468244.185.ПД.01

ЗМІСТ

1 ПРИЗНАЧЕННЯ КОМПЛЕКСУ	4
2 ОПИС КОМПЛЕКСУ	7
2.1 Структура комплексу та призначення технічних засобів.....	7
2.1.1 Сервери ЦСК	7
2.1.2 Сервери взаємодії	8
2.1.3 Сервер моніторингу та синхронізації часу.....	8
2.1.4 Дисковий масив	8
2.1.5 Обладнання синхронізації часу (GPS-приймач)	8
2.1.6 Обладнання повідомлення адміністраторів (GSM-модуль).....	8
2.1.7 Міжмережний екран	8
2.1.8 Мережні криптомодулі	8
2.1.9 Криптомодулі	8
2.1.10 Комутатори.....	9
2.1.11 РС генерації ключів користувачів.....	9
2.1.13 РС обслуговуючого персоналу	9
2.2 Опис функціонування комплексу	10
2.2.1 Порядок взаємодії технічних засобів	10
2.2.2 Інформаційні повідомлення, що передаються між технічними засобами комплексу.....	10
3 ВЗАЄМОДІЯ КОМПЛЕКСУ З ІНШИМИ СИСТЕМАМИ	14

ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ВОЛЗ	- Волоконно-оптичні лінії зв'язку
ДБЖ	- Джерело безперебійного живлення
ЕОМ	- Електронно-обчислювальна машина
ЕОТ	- Електронно-обчислювальна техніка
ЕЦП	- Електронний цифровий підпис
ЄСПД	- Єдина система програмної документації
ЗТМ	- Зовнішні телекомунікаційні мережі
ІТС	- Інформаційно-телекомунікаційна система
КЗЗ	- Комплекс засобів захисту
КЗІ	- Криптографічний захист інформації
КТЗ	- Комплекс технічних засобів
КСЗІ	- Комплексна система захисту інформації
ЛОМ	- Локальна обчислювальна мережа
МЕ	- Міжмережний екран
НКІ	- Носій ключової інформації
НМС	- Накопичувач на магнітній стрічці
ОС	- Операційна система
ПЕОМ	- Персональна ЕОМ
ПЗ	- Програмне забезпечення
ПЗП	- Постійний запам'ятовуючий пристрій
ПРД	- Правила розмежування доступу
ПТК	- Програмно-технічний комплекс
РС	- Робоча станція
СУБД	- Система управління базами даних
ТЗІ	- Технічний захист інформації
ЦСК	- Центр сертифікації ключів
СМР	- Control Messages Protocol (протокол управляючих повідомлень)
GPS	- Global Positioning System (глобальна система позиціонування)
HTTP	- Hyper Text Transfer Protocol
LDAP	- Lightweight Directory Access Protocol (протокол доступу до каталогу)
MTA	- Mail Transfer Agent (модуль передачі електронних поштових повідомлень)
OCSP	- Online Certificate Status Protocol (протокол визначення статусу сертифіката)
TSP	- Time-Stamp Protocol (протокол отримання позначок часу)

1 ПРИЗНАЧЕННЯ КОМПЛЕКСУ

Комплекс призначений для реалізації центром сертифікації ключів (ЦСК) регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів ЦСК (далі - користувачів), надання послуг фіксування часу, надання користувачам засобів ЕЦП та шифрування, а також засобів генерації особистих і відкритих ключів.

Комплекс забезпечує реалізацію регламентних процедур та механізмів роботи ЦСК, пов'язаних з:

- обслуговуванням сертифікатів відкритих ключів (далі - сертифікатів) користувачів, що включає:
 - реєстрацію користувачів;
 - сертифікацію відкритих ключів користувачів;
 - розповсюдження сертифікатів;
 - управління статусом сертифікатів;
 - розповсюдження інформації про статус сертифікатів;
- наданням послуг фіксування часу;
- реалізацією ЕЦП і шифрування даних та управління особистими ключами і сертифікатами користувачів

Комплекс забезпечує виконання наступних функцій, пов'язаних з обслуговуванням ЦСК сертифікатів користувачів:

- реєстрація користувачів, що включає:
 - введення реєстраційних даних користувачів до реєстру користувачів;
 - зберігання реєстру користувачів та забезпечення доступу до реєстраційних даних;
 - резервне копіювання та архівування реєстру користувачів;
 - зміну реєстраційних даних користувачів у реєстрі;
 - видалення реєстраційних даних користувачів з реєстру.
- сертифікація відкритих ключів користувачів, що включає:
 - приймання та реєстрацію запитів користувачів на формування сертифікатів;
 - зберігання запитів, отриманих від користувачів, у базі даних запитів;
 - архівування бази даних запитів;
 - формування сертифікатів користувачів;
 - внесення сформованих сертифікатів у реєстр сертифікатів;
 - зберігання реєстру сертифікатів;
 - архівування реєстру сертифікатів.
- розповсюдження сертифікатів відкритих ключів користувачів, що включає:
 - публікацію реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);
 - забезпечення доступу користувачів до реєстру сертифікатів на інформаційному ресурсі ЦСК.
- управління статусом сертифікатів відкритих ключів користувачів та розповсюдження інформації про статус сертифікатів, що включає:
 - приймання та реєстрацію запитів користувачів на скасування, блокування чи поновлення сертифікатів;
 - зберігання запитів, отриманих від користувачів, у базі даних запитів;
 - архівування бази даних запитів;
 - скасування, блокування або поновлення сертифікатів на основі запитів;
 - внесення інформації про поточний статус сертифіката до реєстру сертифікатів;
 - формування списків відкликаних сертифікатів користувачів;
 - публікацію списків відкликаних сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);
 - забезпечення доступу користувачів до списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;

- забезпечення доступу користувачів до інформації про статус сертифікатів (та самих сертифікатів) з використанням протоколу визначення статусу сертифіката (OCSP).

Комплекс забезпечує виконання наступних функцій, пов'язаних з наданням ЦСК послуг фіксування часу:

- приймання та реєстрацію запитів користувачів на формування позначок часу;
- формування позначок часу;
- передачу сформованих позначок часу користувачам;
- внесення сформованих позначок часу у базу даних;
- зберігання сформованих позначок у базі даних;
- архівування бази даних позначок часу.

Для забезпечення функціонування ЦСК комплекс також виконує такі функції:

- управління ключами ЦСК, що включає:
 - генерацію особистого та відкритого ключів ЦСК;
 - введення та використання особистого ключа ЦСК;
 - створення резервних копій особистого ключа ЦСК, а також відновлення особистого ключа з резервних копій;
 - формування та передачу запиту на формування сертифіката ЦСК до ЦЗО;
 - отримання та запис сформованого сертифікату у реєстр сертифікатів;
 - публікацію сформованого сертифікату на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці).
- ведення реєстру посадових осіб ЦСК (адміністраторів), що включає:
 - введення реєстраційних даних посадових осіб до реєстру посадових осіб;
 - зберігання реєстру посадових осіб та забезпечення доступу до реєстраційних даних;
 - зміну реєстраційних даних посадових осіб у реєстрі;
 - видалення реєстраційних даних посадових осіб з реєстру.
- управління ключами посадових осіб ЦСК (адміністраторів), що включає:
 - генерацію особистого та відкритого ключів посадових осіб;
 - введення та використання особистих ключів посадових осіб;
 - формування та передачу запиту на формування сертифіката посадової особи до ЦСК;
 - формування сертифікату посадової особи;
 - запис сформованого сертифікату у реєстр сертифікатів;
 - отримання, зберігання та використання сертифікату посадовою особою.
- забезпечення адміністрування окремих апаратних та програмних засобів комплексу, що включає:
 - налагодження параметрів засобів комплексу;
 - діагностування роботи засобів комплексу;
 - моніторинг стану засобів комплексу.
- ведення журналів реєстрації окремими технічними засобами комплексу, що включає:
 - запис реєстраційної інформації засобами комплексу до журналів реєстрації;
 - збір та аналіз реєстраційної інформації у журналах.
- забезпечення захисту інформації, що обробляється у комплексі, від НСД.

До складу комплексу також входять засоби користувачів у складі:

- засобів управління особистими ключами і сертифікатами користувачів, які призначені для:
 - генерації особистого та відкритого ключів користувача;
 - формування та передачу запиту на формування сертифіката до ЦСК;
 - отримання, перевірку, зберігання та використання сформованого сертифікату;
 - формування та передачу запитів на блокування, скасування та поновлення сертифіката користувача до ЦСК.
- засобів ЕЦП та шифрування даних, які призначені для:

- введення та використання особистих ключів користувачів;
- пошук та перевірку статусу сертифікатів у файлових сховищах з використанням списків відкликаних сертифікатів (в т.ч. і перевірку ланцюжка сертифікатів - користувача, ЦСК та ЦЗО);
- пошуку сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК);
- пошук та інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК);
- отримання позначок часу у ЦСК (через TSP-сервер ЦСК);
- інтеграції механізмів формування та перевіряння ЕЦП, автентифікації та шифрування даних у системі (програмних засобах АІС).

2 ОПИС КОМПЛЕКСУ

2.1 Структура комплексу та призначення технічних засобів

До складу комплексу входять такі технічні засоби:

- центральні сервери (сервери ЦСК) (кластер);
- сервери взаємодії (кластер);
- сервер моніторингу та синхронізації часу;
- дисковий масив;
- обладнання синхронізації часу (GPS-приймач);
- обладнання сповіщення адміністраторів (GSM-модуль);
- міжмережний екран (далі - ME);
- мережні криптомодулі (кластер);
- криптомодулі;
- комутатори (ЛОМ та PC);
- PC генерації ключів користувачів (ізолювана);
- PC обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації).

Структура КТЗ наведена на структурній схемі КТЗ (документ ЄААД.468244.185.С1).

Функціональна структура комплексу наведена на схемі функціональної структури (документ ЄААД.468244.185.С2).

Детальний опис та характеристики КТЗ (засобів ЕОТ та комунікаційного обладнання) наведений у описі КТЗ (документ ЄААД.468244.185.П9.01).

Детальний опис програмного забезпечення наведений у описі програмного забезпечення (документ ЄААД.468244.185.ПА.01).

2.1.1 Сервери ЦСК

Центральні сервери (сервери ЦСК) призначені для:

- публікації сертифікату ЦСК на інформаційному ресурсі (у LDAP-каталозі);
- зберігання реєстру посадових осіб (адміністраторів) та забезпечення доступу до реєстраційних даних;
- використання реєстру посадових осіб;
- перевірки реєстраційних даних користувачів шляхом перевірки унікальності розпізнавального імені користувача;
- зберігання реєстру користувачів та забезпечення використання реєстраційних даних;
- використання реєстру користувачів;
- резервного копіювання та архівування реєстру користувачів;
- приймання та реєстрації запитів на формування сертифікатів користувачів та посадових осіб (адміністраторів);
- зберігання запитів на формування сертифікатів у базі даних запитів;
- архівування бази даних запитів на формування сертифікатів;
- перевірки унікальності відкритих ключів користувачів;
- зберігання реєстру сертифікатів;
- використання реєстру сертифікатів;
- автоматизованого резервного копіювання та архівування реєстру сертифікатів;
- публікації реєстру сертифікатів на інформаційному ресурсі ЦСК;
- приймання та реєстрації запитів користувачів і адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів;
- зберігання запитів на скасування, блокування чи поновлення сертифікатів у базі даних запитів;
- архівування бази даних запитів на скасування, блокування чи поновлення сертифікатів;
- скасування, блокування або поновлення сертифікатів на основі запитів;
- внесення інформації про поточний статус сертифіката до реєстру сертифікатів;
- публікації списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;

- приймання через сервер взаємодії та обробку запитів користувачів на визначення статусу сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP), шляхом формування інформації про статус сертифікатів;
- приймання через сервер взаємодії та обробку запитів користувачів на формування позначок часу, шляхом формування позначок часу та передачу сформованих позначок часу користувачам;
- внесення сформованих позначок часу у базу даних;
- зберігання сформованих позначок у базі даних;
- архівування бази даних позначок часу.

2.1.2 Сервери взаємодії

Сервери взаємодії призначені для:

- приймання та передачі запитів користувачів та адміністраторів реєстрації на формування сертифікатів користувачів на центральний сервер;
- забезпечення доступу користувачів до реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);
- приймання та передачі запитів користувачів та віддалених адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів користувачів на центральний сервер;
- забезпечення доступу користувачів до списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;
- забезпечення доступу користувачів до інформації про статус сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP), шляхом приймання та передачі запитів на визначення статусу сертифіката на центральний сервер та передачі інформації про статус у зворотному напрямку;
- приймання та передачі запитів користувачів на формування позначок часу на центральний сервер;
- передачі сформованих на центральному сервері позначок часу користувачам;
- забезпечення доступу до сертифікату ЦСК на інформаційному ресурсі.

2.1.3 Сервер моніторингу та синхронізації часу

Сервер моніторингу та синхронізації часу призначений для:

- отримання сигналів точного часу від GPS-приймача;
- синхронізації часу на інших серверах та PC з Всесвітнім координованим часом (NTP-сервер);
- контролю функціонування інших компонентів ЦСК;
- повідомлення адміністраторів ЦСК за допомогою SMS-повідомлень.

2.1.4 Дисковий масив

Дискові масиви призначені для зберігання даних серверів ЦСК.

2.1.5 Обладнання синхронізації часу (GPS-приймач)

Обладнання синхронізації часу (GPS-приймач) призначене для отримання і передачі на сервер моніторингу та синхронізації часу сигналів точного часу.

2.1.6 Обладнання повідомлення адміністраторів (GSM-модуль)

Обладнання повідомлення адміністраторів (GSM-модуль) призначене для отримання передачі повідомлень адміністраторам ЦСК за допомогою SMS-повідомлень.

2.1.7 Міжмережний екран

МЕ з IPS призначені для фільтрації мережного трафіку між телекомунікаційними мережами та сервером взаємодії. Детально функції МЕ з IPS повинні визначатися у ТЗ на КСЗІ ЦСК.

2.1.8 Мережні криптомодулі

Мережні криптомодулі призначені для зберігання особистих ключів серверів ЦСК та формування ЕЦП з їх використанням без необхідності передавати особисті ключі серверів ЦСК за межі криптомодулів.

2.1.9 Криptomодулі

Криptomодулі призначені для зберігання особистих ключів ЦСК та формування ЕЦП з їх використанням без необхідності передавати особисті ключі серверів ЦСК за межі криптомодулів.

2.1.10 Комутатори

Комутатори та інше внутрішнє комунікаційне обладнання призначене для забезпечення внутрішньої взаємодії засобів комплексу та утворення ЛОМ.

2.1.11 РС генерації ключів користувачів

РС генерації ключів користувачів призначена для:

- генерації особистого та відкритого ключів користувача та запис особистого ключа на носій ключової інформації (НКИ);
- формування та запису на носій інформації запиту на формування сертифіката користувача.

2.1.13 РС обслуговуючого персоналу

2.1.13.1 РС адміністратора безпеки призначена для:

- введення реєстраційних даних посадових осіб (адміністраторів) до реєстру посадових осіб;
- зміну реєстраційних даних посадових осіб у реєстрі;
- видалення реєстраційних даних посадових осіб з реєстру;
- виконання інших функцій, пов'язаних із забезпеченням та підтримкою безпеки інформації, що обробляється у комплексі. Детально вимоги до призначення РС адміністратора безпеки повинні визначатися у ТЗ на КСЗІ ЦСК.

2.1.13.2 РС системного адміністратора призначена для:

- налагодження параметрів технічних засобів комплексу та системного програмного забезпечення;
- діагностування роботи технічних засобів комплексу;
- моніторингу та контролю стану технічних засобів комплексу та виконання ним окремих функцій.

2.1.13.3 РС системного адміністратора призначена для:

РС адміністратора реєстрації призначена для:

- генерації особистого та відкритого ключів адміністратора реєстрації;
- передачі запиту на формування сертифіката адміністратора реєстрації на центральний сервер;
- отримання, зберігання та використання сертифікату адміністратора реєстрації;
- введення та використання особистого ключа адміністратора реєстрації;
- введення реєстраційних даних користувачів до реєстру користувачів;
- зміни реєстраційних даних користувачів у реєстрі;
- видалення реєстраційних даних користувачів з реєстру;
- приймання запитів користувачів на формування сертифікатів, що включає перевірку володіння користувачем особистого ключа, відповідного до відкритого ключа у запиті;
- ініціювання формування сертифікатів користувачів шляхом ведення та передачі запитів користувачів на формування сертифікатів до центрального сервера, що включає підпис запитів користувачів адміністратором (з використанням особистого ключа адміністратора);
- ініціювання скасування, блокування чи поновлення сертифікатів користувачів шляхом ведення та передачі запитів на зміну статусу сертифікатів до центрального сервера, що включає підпис запитів адміністратором (з використанням його особистого ключа).

2.1.13.4 РС адміністратора сертифікації призначена для:

- генерації особистого та відкритого ключів ЦСК;
- введення та використання особистого ключа ЦСК;
- створення резервних копій особистого ключа ЦСК, а також відновлення особистого ключа з резервних копій;
- формування та передачі запиту на формування сертифіката ЦСК до ЦЗО;
- отримання та запису сертифікату ЦСК у реєстр сертифікатів;
- публікації сертифікату ЦСК на інформаційному ресурсі (на веб-сторінці сервера взаємодії);
- публікації списків відкликаних сертифікатів на інформаційному ресурсі ЦСК (на веб-сторінці);
- приймання запитів на формування сертифікатів користувачів та посадових осіб (адміністраторів);

- формування сертифікатів на основі запиту шляхом, що включає підпис сертифікатів (з використанням особистого ключа ЦСК);
- формування списків відкликаних сертифікатів користувачів шляхом, що включає підпис списків відкликаних сертифікатів (з використанням особистого ключа ЦСК);
- ручного резервного копіювання та архівування реєстру сертифікатів;
- моніторингу та контролю виконання автоматизованих функцій, зокрема:
 - публікації реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці) центральний сервером;
 - публікації списків відкликаних сертифікатів на інформаційному ресурсі центральним сервером;
 - публікації сертифікату ЦСК на інформаційному ресурсі центральним сервером.

2.2 Опис функціонування комплексу

2.2.1 Порядок взаємодії технічних засобів

Порядок взаємодії технічних засобів при виконанні функціональних завдань наведено на схемі функціональної структури (ЄААД.468244.185.С2).

Взаємодія технічних засобів комплексу у ЛОМ здійснюється через комутатори ЛОМ та РС. Взаємодія із зовнішніми ІТС користувачів здійснюється через сервер взаємодії (функціонально) та МЕ підключений до обладнання оператора передачі даних (фізично) у зовнішніх телекомунікаційних мережах.

2.2.2 Інформаційні повідомлення, що передаються між технічними засобами комплексу

Інформацію щодо типу та формату інформаційних повідомлень, що передаються між технічними засобами комплексу наведено у табл. 2.1.

Таблиця 2.1 - Інформаційні повідомлення, що передаються між технічними засобами комплексу.

Задіяні технічні засоби	Призначення та характеристики повідомлень, що передаються
РС адміністратора безпеки Центральні сервери, сервери взаємодії, сервер моніторингу та синхронізації часу	Призначення: Налагодження параметрів ПЗ та технічних засобів (серверів ЦСК). Налагодження параметрів КЗЗ ПЗ та технічних засобів. Аналіз журналів реєстрації. Технологічні повідомлення про стан функціонування та захищеності. Протоколи: RDP (3389), SQL на основі TCP. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та РС адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
РС адміністратора безпеки Сервери взаємодії	Призначення: Налагодження параметрів ПЗ та технічних засобів (серверів взаємодії). Налагодження параметрів КЗЗ ПЗ та технічних засобів. Аналіз журналів реєстрації. Технологічні повідомлення про стан функціонування та захищеності. Протоколи: SSH, HTTPS. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та РС адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
Сервери ЦСК РС адміністратора реєстрації	Призначення: Формування сертифікатів на сервері ЦСК (сервері обробки запитів). Зміна статусу сертифікатів на сервері ЦСК (сервері обробки запитів). Формати: PKCS#10, запити на зміну статусу (CCSR) інкапсульовані у запити на управління (CMP). Протоколи: CMP на основі TCP. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та РС адміністраторів

Задіяні технічні засоби	Призначення та характеристики повідомлень, що передаються
	передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
Центральні сервери PC адміністратора реєстрації	Призначення: Робота з БД сертифікатів та облікових записів користувачів. Формати: SQL. Протоколи: SQL на основі TCP. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та PC адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
PC системного адміністратора Сервер ЦСК (БД)	Призначення: Доступ до БД. Адміністрування БД. Формати: SQL. Протоколи: SQL на основі TCP. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та PC адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
PC системного адміністратора Сервер взаємодії ЦСК	Призначення: Доступ до LDAP каталогу. Адміністрування LDAP сервера. Публікація сертифікатів та CBC у LDAP-каталог. Протоколи: LDAP. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та PC адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
PC системного адміністратора Сервер взаємодії ЦСК	Призначення: Публікація сертифікатів та CBC на web-сторінку сервера взаємодії (HTTP-сервера). Запис інформації на web-сторінку сервера взаємодії (HTTP-сервера). Адміністрування HTTP сервера. Протоколи: HTTP на основі TCP. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та PC адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
PC системного адміністратора Центральні сервери	Призначення: Формування повних та часткових CBC на сервері ЦСК (сервері обробки запитів). Формати: запити на управління (CMP). Протоколи: CMP на основі TCP. Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та PC адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).
Сервер взаємодії ЦСК Центральні сервери	Призначення: Передача запитів на створення, блокування, скасування сертифікатів тощо, від віддалених адміністраторів реєстрації, користувачів. Протоколи: CMP на основі TCP.
Сервер взаємодії ЦСК Центральні сервери	Призначення: Передача запитів на отримання статусу сертифікатів.

Задіяні технічні засоби	Призначення та характеристики повідомлень, що передаються
	<p>Формати: OCSP-запити та відповіді.</p> <p>Протоколи: OCSP на основі TCP.</p>
Сервер взаємодії ЦСК Центральні сервери	<p>Призначення: Передача запитів на отримання позначок часу.</p> <p>Формати: TSP-запити та відповіді.</p> <p>Протоколи: TSP на основі TCP.</p>
PC адміністратора безпеки Комутатор ЛОМ	<p>Налагодження параметрів технічних засобів (комутатор). Аналіз журналів реєстрації. Технологічні повідомлення про стан функціонування та захищеності.</p>
PC адміністратора безпеки ME	<p>Налагодження параметрів технічних засобів (міжмережевий екран). Аналіз журналів реєстрації. Технологічні повідомлення про стан функціонування та захищеності.</p> <p>Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та PC адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).</p>
PC адміністратора безпеки Мережеві криптомодулі	<p>Налагодження параметрів технічних засобів (мережеві криптомодулі). Резервне копіювання ключів. Відновлення ключів. Технологічні повідомлення про стан функціонування та захищеності.</p> <p>Передача даних здійснюється через сервер доступу адміністраторів. Дані між сервером доступу адміністраторів та PC адміністраторів передаються у захищеному вигляді (захист даних на рівні Ethernet протоколу).</p>
Сервери взаємодії Технічні засоби користувачів ЦСК	<p>Призначення: Зміна статусу (блокування) сертифікатів (транзакційні запити та відповіді для передачі на сервер ЦСК). Визначення статусу сертифікатів (транзакційні запити та відповіді для передачі на сервер ЦСК). Формування позначок часу (транзакційні запити та відповіді для передачі на сервер ЦСК).</p> <p>Формати: PKCS#10, запити на зміну статусу (CCSR) інкапсульовані у запити на управління (CMP), OCSP- і TSP-запити та відповіді.</p> <p>Протоколи: CMP, OCSP та TSP на основі HTTP.</p>
Сервери взаємодії Технічні засоби користувачів ЦСК	<p>Призначення: Зміна статусу (блокування) сертифікатів (транзакційні запити та відповіді для передачі на сервер ЦСК).</p> <p>Формати: запити на зміну статусу (CCSR) інкапсульовані у запити на управління (CMP).</p> <p>Протоколи: CMP у вигляді вкладень поштових повідомлень - SMTP та POP3.</p>
Сервери взаємодії Технічні засоби користувачів ЦСК	<p>Призначення: Доступ до LDAP-каталогу сервера взаємодії (LDAP-сервера).</p> <p>Протоколи: LDAP.</p>
Сервери взаємодії Технічні засоби користувачів ЦСК	<p>Призначення: Доступ до web-сторінки сервера взаємодії (HTTP -сервера).</p> <p>Протоколи: HTTP.</p>
Центральні сервери ЦСК МКМ	<p>Передача даних для виконання операцій шифрування та підпису у мережевому криптомодулі.</p>

Задіяні технічні засоби	Призначення та характеристики повідомлень, що передаються
	Протоколи: TCP.
Центральні сервери ЦСК МКМ	Передача даних для виконання операцій шифрування та підпису у мережевому криптомодулі. Протоколи: TCP.
Центральні сервери ЦСК МКМ	Передача даних для виконання операцій шифрування та підпису у мережевому криптомодулі. Протоколи: TCP.
Центральні сервери ЦСК МКМ	Передача даних для виконання операцій шифрування та підпису у мережевому криптомодулі. Протоколи: TCP.
Сервер моніторингу та синхронізації часу Центральні сервери ЦСК, сервери взаємодії	Синхронізація часу на інших серверах та PC Протоколи: NTP
Сервер моніторингу та синхронізації часу Центральні сервери ЦСК, сервери взаємодії, мережні криптомодулі	Контроль функціонування Протоколи: SNMP, ICMP

3 ВЗАЄМОДІЯ КОМПЛЕКСУ З ІНШИМИ СИСТЕМАМИ

Комплекс під час функціонування взаємодіє з технічними засобами користувачів ЦСК з зовнішніх ІТС.

Взаємодія здійснюється через зовнішні (по відношенню до комплексу) телекомунікаційні мережі. При цьому взаємодія здійснюється через комутатор що програмується.

Фізично взаємодія здійснюється через МЕ та комунікаційне обладнання.